AMENDMENTS TO THE CLAIMS

1-50. (Canceled)

51. (New) A method in a server computer system of authenticating client computer systems using various authentication mechanisms, the method comprising:

receiving from a controlling client computer system a first instruction identifying a first client computer system, identifying a first information related to the controlling client computer system available to the first client computer system through a service of the server computer system, and identifying at least one first authentication mechanism that can be used to authenticate the first client computer system, the first authentication mechanism specifying at least one first type of information necessary to verify a first purported identity of the first client computer system, the first client computer system having client-specific knowledge of the information necessary to verify the first purported identity of the first client computer system, the first client computer system being separate from the controlling client computer system;

receiving from the controlling client computer system a second instruction identifying a second client computer system, identifying a second information related to the controlling client computer system available to the second client computer system through the service of the server computer system, identifying a second authentication mechanism that can be used to authenticate the second client computer system, and identifying a third authentication mechanism that can be used to authenticate the second client computer system, the second authentication mechanism specifying a second type of information necessary to verify a second purported identity of the second client computer system, the second client computer system having client-specific knowledge of the information necessary to verify the second purported identity of the second client computer system, the third

authentication mechanism specifying a third type of information necessary to verify a third purported identity of the second client computer system, the second client computer system having client-specific knowledge of the information necessary to verify the third purported identity of the second client computer system, the second client computer system being separate from the controlling client computer system;

storing, for the first client computer system, an indication of the first authentication mechanism;

storing, for the second client computer system, an indication of the second authentication mechanism and the third authentication mechanism;

after receiving the first instruction and before authenticating the first client computer system, receiving a first request from the first client computer system to access the service of the server computer system, the first request including information of the type specified by the first authentication mechanism that is necessary to verify the first purported identity of the first client computer system, wherein the information is known specifically to the first client computer system;

initially authenticating the first client computer system using the first authentication mechanism based on the information received from the first client computer system that is necessary to verify the first purported identity of the first client computer system;

after receiving the second instruction and before authenticating the second client computer system, receiving a second request from the second client computer system to access the service of the server computer system;

upon receiving the second request from the second client computer system to access the service of the server computer system, selecting a selected authentication mechanism from the second and third authentication mechanisms, the selected authentication mechanism being different from the first authentication mechanism; and

authenticating the second client computer system using the selected authentication mechanism based on information received from the second client computer system that is necessary to verify the second or third purported identity of the second client computer system corresponding to the selected authentication mechanism.

52. (New) The method of claim 51 wherein selecting the selected authentication mechanism is based on an ability of the server computer system to support the second and third authentication mechanisms and access rights of the second client computer system to access resources of the service of the server computer system.

53. (New) The method of claim 51 wherein the second request includes information of the type specified by the third authentication mechanism that is necessary to verify the third purported identity of the second client computer system, wherein the information is known specifically to the second client computer system, the method further comprising initially authenticating the second client computer system using the third authentication mechanism based on the information received from the second client computer system that is necessary to verify the third purported identity of the second client computer system.

54. (New) The method of claim 53, wherein the third authentication mechanism is the same as the first authentication mechanism.

55. (New) The method of claim 51 wherein the selected authentication mechanism includes an assertion authentication, and wherein the type of information specified by the assertion authentication is an indication of an identity of the second client computer system.

56. (New) The method of claim 51 wherein the selected authentication mechanism includes a basic HTTP authentication, and wherein the type of information specified by the basic HTTP authentication is a password of the second client computer system.

57. (New) The method of claim 51 wherein the selected authentication mechanism includes digest authentication, and wherein the type of information specified by the digest authentication is a digest generated by hashing a series of numbers associated with the second client computer system.

58. (New) The method of claim 51 wherein the selected authentication mechanism includes an NTLM authentication, and wherein the type of information specified by the NTLM authentication comprises credentials of the second client computer system, wherein the credentials include a user name and an encrypted password of the second client computer system.

59. (New) A method in a controlling client computer system for providing indications of authentication mechanisms to a server computer system, the method comprising:

generating a first instruction identifying a first client computer system, identifying a first resource of information related to the controlling client computer system of a service of the server computer system, and identifying a first authentication mechanism that can be used to authenticate the first client computer system, the first authentication mechanism specifying a type of information necessary to verify a purported identity of the first client computer system, the first client computer system having client-specific knowledge of the information necessary to verify the purported identity of the first client computer system, the first client computer system being different from the controlling client computer system;

generating a second instruction identifying a second client computer system, identifying a second resource of information different from the first resource of information and related to the controlling client computer system of the service of the server computer system, and identifying a second authentication mechanism different from the first authentication mechanism that can be used to authenticate the second client computer system, the second authentication mechanism specifying a type of information necessary to verify a purported identity of the second client computer system, the second client computer system having client-specific knowledge of the information necessary to verify the purported identity of the second client computer system, the second client computer system being different from the controlling client computer system; and

sending the first and second instructions to the server computer system so that upon receiving a first request from the first client computer system to access information related to the controlling client computer system through the service of the server computer system, after the first instruction is received at the server computer system, the server computer authenticates the first client computer using the first authentication mechanism and provides the first resource of information to the first client computer based on the first instruction, and upon receiving a second request from the second client computer system to access information related to the controlling client computer system through the service of the server computer system, after the second instruction is received at the server computer system, when the second client computer system can be authenticated using multiple authentication mechanisms, the server computer system selects a selected authentication mechanism based on authentication abilities of the second client computer system to support the selected authentication mechanism, authentication abilities of the server computer system to support the selected authentication mechanism, and access rights of the second client computer

system to access information related to the controlling client computer system, the server computer system initially authenticates the second client computer system using the selected authentication mechanism based on information received from the second client computer system that is necessary to verify the purported identity of that client computer system, and in response to the authentication of the second client computer system, the server computer system provides the second resource of information.

60. (New) The method of claim 59 wherein a plurality of instructions indicate that the same authentication mechanism is to be used to authenticate multiple client computer systems when associated with the same resource of information related to the controlling client computer, and wherein the multiple client computer systems are authenticated by the server computer system using the indicated authentication mechanism.

61. (New) The method of claim 59 wherein the selected authentication mechanism includes an assertion authentication, and wherein the type of information specified by the assertion authentication is an indication of an identity of the second client computer system.

62. (New) The method of claim 59 wherein the selected authentication mechanism includes a basic HTTP authentication, and wherein the type of information specified by the basic HTTP authentication is a password of the second client computer system.

63. (New) The method of claim 59 wherein the selected authentication mechanism includes digest authentication, and wherein the type of information specified by the digest authentication is a digest generated by hashing a series of numbers associated with the second client computer system.

64. (New) The method of claim 59 wherein the selected authentication mechanism includes an NTLM authentication, and wherein the type of information specified by the NTLM authentication comprises credentials of the second client computer system, wherein the credentials include a user name and an encrypted password of the second client computer system.

65. (New) A tangible computer-readable medium containing instructions for controlling a server computer system to authenticate entities using various authentication mechanisms, by a method comprising:

receiving from a controlling client computer system a first instruction identifying a first client computer system, identifying a first information related to the controlling client computer system available to the first client computer system through a service of the server computer system, and identifying at least one first authentication mechanism that can be used to authenticate the first client computer system, the first authentication mechanism specifying at least one first type of information necessary to verify a first purported identity of the first client computer system, the first client computer system having client-specific knowledge of the information necessary to verify the first purported identity of the first client computer system, the first client computer system being separate from the controlling client computer system;

receiving from the controlling client computer system a second instruction identifying a second client computer system, identifying a second information related to the controlling client computer system available to the second client computer system through the service of the server computer system, identifying a second authentication mechanism that can be used to authenticate the second client computer system, and identifying a third authentication mechanism that can be used to authenticate the second client computer system, the second authentication mechanism specifying a second type of information necessary to verify a second purported identity of the

second client computer system, the second client computer system having client-specific knowledge of the information necessary to verify the second purported identity of the second client computer system, the third authentication mechanism specifying a third type of information necessary to verify a third purported identity of the second client computer system, the second client computer system having client-specific knowledge of the information necessary to verify the third purported identity of the second client computer system, the second client computer system being separate from the controlling client computer system;

storing, for the first client computer system, an indication of the first authentication mechanism;

storing, for the second client computer system, an indication of the second authentication mechanism and the third authentication mechanism;

after receiving the first instruction and before authenticating the first client computer system, receiving a first request from the first client computer system to access the service of the server computer system, the first request including information of the type specified by the first authentication mechanism that is necessary to verify the first purported identity of the first client computer system, wherein the information is known specifically to the first client computer system;

initially authenticating the first client computer system using the first authentication mechanism based on the information received from the first client computer system that is necessary to verify the first purported identity of the first client computer system;

after receiving the second instruction and before authenticating the second client computer system, receiving a second request from the second client computer system to access the service of the server computer system;

upon receiving the second request from the second client computer system to access the service of the server computer system, selecting a selected

authentication mechanism from the second and third authentication mechanisms, the selected authentication mechanism being different from the first authentication mechanism; and

authenticating the second client computer system using the selected authentication mechanism based on information received from the second client computer system that is necessary to verify the second or third purported identity of the second client computer system corresponding to the selected authentication mechanism.

66. (New) The computer-readable medium of claim 65 wherein selecting the selected authentication mechanism is based on an ability of the server computer system to support the second and third authentication mechanisms and access rights of the second client computer system to access resources of the service of the server computer system.

67. (New) The computer-readable medium of claim 65 wherein the second request includes information of the type specified by the third authentication mechanism that is necessary to verify the third purported identity of the second client computer system, wherein the information is known specifically to the second client computer system, the method further comprising initially authenticating the second client computer system using the third authentication mechanism based on the information received from the second client computer system that is necessary to verify the third purported identity of the second client computer system.

68. (New) The computer-readable medium of claim 65, wherein the third authentication mechanism is the same as the first authentication mechanism.

69. (New) The computer-readable medium of claim 65 wherein the selected authentication mechanism is a member of a group consisting of an assertion

authentication, a basic HTTP authentication, a digest authentication, and an NTLM authentication.